Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

Research Challenges

April 2006

A Report from the Financial Services Sector Coordinating Council

Research Challenges

The Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (the "FSSCC" http://www.fsscc.org) wishes to support research and development initiatives to ensure the protection and resilience of the physical and electronic information of Banking and Finance activities that are vital to the nation's economic well-being. For this purpose the FSSCC has established a Research and Development Committee (the "Committee") as a standing committee to coordinate these activities on behalf of the financial services sector.

The Committee's mission statement calls for the creation of a FSSCC R&D Agenda to identify and prioritize areas of need, in which the most promising opportunities can be found for research, and development initiatives to significantly improve the Financial Services Sector's Critical Infrastructure Protection, and to provide Industry, Research/Academia and the public with a shared insight into the opportunities and requirements.

Table of Contents

2 Acknowledgements

3 Challenge Project 1: Secure Financial Transaction Protocol (SFTP)

5 Challenge Project 2: Resilient Financial Transaction System (RFTS)

7 Challenge Project 3: Enrollment and Identity Credential Management

10 Challenge Project 4: Suggested Practices and Standards

13 Challenge Project 5: Understanding and Avoiding the Insider Threat

16 Challenge Project 6: Financial Information Tracing and Policy Enforcement

18 Challenge Project 7: Testing

21 Challenge Project 8: Standards for measuring ROI of CIP and Security Technology

22 Role of the Branding & Finance Test Bed

Acknowledgements

This paper has been developed based primarily on an earlier paper entitled Closing the Gap: A Research and Development Agenda to Improve the Resiliency of the Financial and Banking Sector by Dr. Jerrold M. Grochow of MITRE Corporation and the Massachusetts Institute of Technology with the support of Deputy Assistant Secretary D. Scott Parsons and also of Brian Peretti, both of the U.S. Department of the Treasury, Office of Critical Infrastructure Protection and Compliance Policy. Significant additional contributions have been made by members of the Committee. These include: Dwight Arthur, C. Warren Axelrod, Andy Bach, Jennifer Bayuk, Larry K. Bickner, John Carlson, Byron Collie, Dan DeWaal, Don Donahue, Gene Fredriksen, David LaFalce, Mark Merkow, John Panchery, Dan Schutzer, and Zachary Tumin. The work was also supported by American Express, Bear, Stearns & Co. Inc., Banking Information Technology Secretariat, ChicagoFIRST, Depository Trust and Clearing Corporation, Financial Services Technology Consortium, Futures Industry Association, Options Clearing Corporation, Pershing, Goldman Sachs & Co., Raymond James, Securities Industry Association, Securities Industry Automation Corporation, and The Clearing House.

Challenge Project 1
Secure Financial Transaction Protocol (SFTP)

The Situation

Modern Financial Services are built on a foundation of information technology, including computing hardware, software and telecommunications. This foundation is afflicted by myriad vulnerabilities and a high and rising level of threats. Many people who devise exploits based on these vulnerabilities choose to attack the systems and networks of the financial services industry because "that's where the money is." Although the Information Technology and Telecommunications industries have responded with Trusted Computing and Secure Network initiatives, the incidence of account takeover, identity theft and other fraudulent acts is increasing, with the bad guys clearly winning. Financial Services must respond by building a secure protocol and infrastructure that can ride on top of the existing untrustworthy foundation.

Impact and timing

The result of these trends, if not checked, would be for customers to lose confidence in the banking system, which has become increasingly compromised by unreliable and insecure networks and systems. If this situation is not addressed within the next 2-5 years, the Banking and Financial Services Industry will face critical brand erosion and significant loss of customers, in addition to losses realized by their customers.

The Challenge

1 Design a Secure Financial Transaction Protocol that enables the transacting parties (be they between Financial Institutions (FI's), or between FI's and their customers) to securely exchange financial information and commands, e.g. account information, payment instructions, with confidence even though the message protocol traverses untrustworthy communications networks and computing nodes. The protocol should:

1.1 Reliably and unambiguously identify the originator of a message.

1.2 Ensure only the intended recipient(s) will be able to receive and understand the message.

1.3 Protect message content against tampering,

Challenge Project 1
Secure Financial Transaction Protocol (SFTP)

and identify any attempt to modify message content.

1.4 Promote interoperability among FI's by use or extend existing industry standards to encode and encrypt message content.

1.5 Support use as a service into any number of diverse Financial Service Applications.

1.6 Scale to support very high transaction rates, on a scale exceeding hundreds of millions of transactions per day, operating globally, 24x7.

Research to support this challenge should include:

- Possible applications of advanced encryption (e.g. Quantum) and stenographic techniques to this problem.

- Development of metrics to measure the effectiveness of a Financial Service protocol.

Challenge Project 2
Resilient Financial Transaction System (RFTS)

The Situation

Modern Financial Services are built on a foundation of information technology, including computing hardware, software and telecommunications. This foundation suffers from an ever-increasing variety of vulnerabilities, including physical attack, cyber attacks, misuse and fraudulent use, and natural disaster. Financial Services must respond by exploring the feasibility of a more secure, flexible and resilient IT foundation.

Impact and timing

The result of these trends, if not checked, would be for customers to lose confidence in the banking system, which has become increasingly compromised by unreliable and insecure networks and systems. If this situation is not addressed within the next 2-5 years, the Banking and Financial Services Industry will face critical brand erosion and significant loss of customers, in addition to losses realized by their customers.

The Challenge

2 Evaluate the architecture of a more secure, more resilient, and more flexible financial transaction system infrastructure. Such an infrastructure should:

2.1 Address secure data replication across great distances.

2.2 Shift load from congested or compromised facilities to other available facilities.

2.3 Support the creation of shared capacity able to absorb demand displaced by a wide variety of incidents.

2.4 Extend connectivity through areas in which basic services are unavailable, using local power generation, rapid deployment of wireless communications, mobile kiosks or other innovative techniques.

2.5 Maintain the economic efficiency of the public communications and commercial off-the-shelf (COTS) computer systems.

Challenge Project 2
Resilient Financial Transaction System (RFTS)

2.6 Provide sufficient redundancy and flexibility to continue operation without significant degradation of services while under cyber and physical attack, or during natural disasters.

Research to support this challenge should include the development of metrics to measure the resilience of a Financial Service System.

Challenge Project 3
Enrollment and Identity Credential Management

The Situation

A secure financial infrastructure demands reliable and unambiguous identification of all parties involved in a transaction, and non-repudiation of authorized transactions. Current technologies offer spot solutions that secure an aspect of identity management but many vulnerabilities remain. The absence of an agreed-upon architectural solution means that vulnerabilities will continue to be discovered, especially as criminal elements are increasingly focused on financial fraud enabled by attacks on identity management.

Impact and timing

There are widely varying estimates of losses due to identity based financial fraud, with some estimates clearly not credible. However, even the lowest estimates are high and rising. A perception of widespread risk of identity-based financial fraud could lead to declining consumer confidence in online banking, resulting in a loss of potential customer activity. This perception could also increase the risk of legislatively mandated sub-optimal solutions.

The Challenge

3 Define the architecture of an "identity layer" suitable for incorporation in all financial services protocols and communications. This identity layer should:

3.1 Provide secure and reliable identification of all parties.

3.2 Provide strong authentication of all parties using existing authentication methods such as biometrics or new methods to be developed.

3.3 Provide a reasonable level non-repudiation of financial transactions undertaken by authenticated participants.

3.4 Preserve identity across all interfaces and protocols.

3.5 Include procedures that verify an applicant's right to enroll under a particular identity.

3.6 Support new approaches to strengthening en-

Challenge Project 3
Enrollment and Identity Credential Management

rollment procedures, including new question-based identification approaches, and investigating and developing new, stronger approaches to identity verification, including the use of biometrics.

3.7 Provide flexibility to incorporate improved methods for an individual who has verified identity with a Financial Institution to use that identity in dealings with other institutions, financial or non-financial, including "trust models" that address liability issues.

Identity management projects must also satisfy the following issues:

- The privacy and confidentiality of identity data and identity management artifacts, such as enrollment questions, must be strictly protected throughout the identity management domain.

- Any technology developed must incorporate privacy and confidentiality protections.

- Research must incorporate the social and psychological issues that affect whether a solution will be acceptable to the public. What factors make a security procedure "feel" intrusive versus reassuring to the public? How can security enhancements be presented in a way that enhances public confidence without causing resentment?

- Risks inherent in advances in identity management must be articulated and documented and methods of mitigating and managing these risks must be identified.

- Proposed research must be able to address a known issue for the industry where the current vulnerabilities and losses can be quantified and the effect of the research in eliminating or reducing these risks can be estimated.

- A framework with more precise terminology to better understand the nature of identity management and the distinctions between identity verification, authentication and authorization, including a more fine grained approach to establishing and managing identity claims and authorizations.

Challenge Project 3

Enrollment and Identity Credential Management

- Metrics to better evaluate and compare various authentication technologies and identity management schemes.

Challenge Project 4
Suggested Practices and Standards

The Situation

One of the prevailing techniques for closing the gap between state-of-the-art and state-of-the-practice is the development of standards and suggested practices, also known as "best practice." In an attempt to further the protection of the Banking and Finance critical infrastructures numerous best practice documents have been developed, most addressing a closely circumscribed segment of Banking and Finance systems and practices. Standards such as Cobit, ISO 17799, GAISP, and ITAA are in development or have been issued. While efforts to promulgate these documents and encourage adoption of these standards have been uneven, this challenge continues to consistently score near the top whenever these R&D opportunities are prioritized. Part of the problem is that, to date, the industry has been unable to quantitatively correlate best practices with reduced risk. If such a relationship could be determined and quantified, Financial Institutions would have the tools needed to justify risk management and risk preventive measures. This analysis could, in turn, assist the industry in agreeing on a common and consistent set of "best practices."

Impact and timing

Inaccessible or uncoordinated standards and best practices and unclear return on investment (ROI) contribute to the gap between state-of-the-art and state-of-the-practice. In this space there are many chronically missed opportunities and the potential for substantial gains based on modest investment.

The Challenge

4 Create a best practices and standards repository and incident database available for members of the financial and banking sector via the web to enable research into the effectiveness and correlation of these best practices to the reduction and management of risk. Industry, enterprise, system and process practices and standards should be sought out, summarized, categorized, indexed, and made available to the community. The Department of Justice standards registry is an example of this (http://it.ojp.gov/jsr/public/index.jsp). Such a repository should include the following topics:

4.1 Enterprise Security Management: enterprise policy definition and management, definition and

Challenge Project 4
Suggested Practices and Standards

maintenance of a targeted risk posture, and definition of, and protection at, security boundaries.

4.2 Integration between physical and IT security systems. The lack of this integration has resulted in organizational and procedural gaps that impede organizations from consistently implementing security policies.

4.3 Improved coordination of security standards across network connections, ensuring security across wired and wireless devices, with particular concern to interoperability and privacy.

4.4 Access control standards, including standards for the expression of authorization policies such as XACML, including practices supportive of the adoption and use of this or similar access control standards.

4.5 Best practices for reducing the gaps in security between financial institutions, merchants, and consumers.

4.6 Best practices regarding outsourcing critical functions, particularly those related to networks and information systems, that address the implications for cyber-security, business continuity, and overall risk management.

4.7 Best practices in Business Continuity Planning, including methods of determining the minimal operational requirements of an organization and strategies for achieving these requirements after a contingency event.

4.8 Best practices in Business Continuity Planning for selecting recovery time objectives (RTO) and recovery point objectives (RPO) for data replication, considering the distance between operational locations, the nature of critical business processes, cost, and sound business practices.

4.9 Standards regarding the ability of key components of the Finance and Banking sector to establish and maintain communication between their various primary and alternate facilities with the capability to conduct transactions at a sufficient volume and level of accuracy.

Challenge Project 4
Suggested Practices and Standards

4.10 Best practices regarding the verification and preservation of physical diversity of telecommunications routing.

4.11 Robust security practices in code development.

4.12 Identification of the key elements of secure software code/products.

4.13 Quantify the impact of "safe practices" on reducing exposure.

4.14 Identify the shared responsibilities of key players and quantify who benefits from good and bad security practices.

This endeavor should also investigate new, innovative technologies that might improve the current state of best practices. For example, explore Decontamination: Unlike a [database] restore operation used to recreate a clean system after a failure, reconstitution [of data after an attack] requires an additional step: decontamination, which is the process of distinguishing clean system state (unaffected by the intruder) from the portions of infected system state, and eliminating the causes of those differences. Because system users would prefer that as little good data as possible be discarded, this problem is quite difficult. Research is needed to create new decontamination approaches for discarding as little good data as possible and for removing active and potential infections on a system that cannot be shut down for decontamination.

Challenge Project 5
Understanding and Avoiding the Insider Threat

The Situation

To operate effectively, Financial Institutions (FI's) must grant employees and contractors access to confidential customer and business information. To establish a measure of trust in this access granting process, Financial Institutions use identity verification, criminal background checking, credit history checking, and other historical data checking approaches to identify and separate the group of untrustworthy individuals, who are denied employment and access, from the group of trustworthy employees and contractors, who are granted access and entitlements based on their job or role in the organization. FI's recognize that current measures provide only a coarse-grained qualification of trust to begin the access granting process. Employees and contractors are then granted access to networks, systems, databases, applications, and ultimately customer and business information based on their job or role in the Institution. Controls on access enforced via a highly complex set of overlapping operational and technical controls. The complexity of these measures is reflected in the fact that a large percentage of each FI's total information protection budget is dedicated to access management, control, and reporting.

Despite the pre-employment/engagement checking processes, and the layering of costly operational and technical controls, FI's continue to experience damage from the unprofessional, malicious, or criminal activities committed by employees and contractors. Examples include:

Unauthorized data duplication and distribution – Employees or contractors create unauthorized copies of customer records and business data as part of legitimate business processes, or to bypass dysfunctional processes, and distribute data to other employees or contractors who are not entitled to the data

Account surfing – Employees and contractors access customer accounts outside of official business purposes

Challenge Project 5
Understanding and Avoiding the Insider Threat

Account/Information extraction and distribution

– Employees or contractors distribute confidential customer or business information to parties outside the Institution

Current approaches suggest adding additional layers surveillance processes and technologies to detect, identify, and help stop the unwanted activities or employees and contactors, but such approaches, while they may reduce undesirable activity, add substantial operating costs to an already costly access management approach. There is also a risk to the National Financial Infrastructure as a coordinated attack by several or several hundred individuals with access into multiple Institutions working as a group with terrorist or criminal goals could cripple the Financial Infrastructure and damage customer confidence, triggering an economic downturn.

Research is needed to determine how to best approach the insider problem at all phases of the employee and contractor activity life cycle, and across all of the phases of the information asset life cycle. Threats can always change faster than layers of control and surveillance complexity can be added to respond; therefore, research should strive for breakthrough thinking to address this problem holistically and from a number of different viewpoints.

Impact and timing

Insider events in individual FI's can damage the reputation of the Institution and, taken as a group, can degrade customer confidence in the entire Financial Infrastructure. Continued problems could cause a downward confidence spiral in which external attacks could become increasingly effective at reducing customer confidence. The insider problem appears to be growing despite increased funding and oversight within FI's and from regulators.

The Challenge

5 Bring together a research team with wide ranging skill sets to accurately and thoroughly identify, measure, and document the personnel/behavioral, operating process/procedural, the technical/technological, policy, and the financial aspects of this problem. The research should:

Challenge Project 5
Understanding and Avoiding the Insider Threat

5.1 Review the scope of operating issues faced by individual FI's, including defining the problem in terms of a coordinated attack on the National Financial Infrastructure.

5.2 Provide a framework for describing and understanding the totality of the insider threat, and to produce or advance a common language for describing the problem in its various forms.

5.3 Provide conclusions about the nature, scope, size, extent, and direction of movement so that FI decision makers can understand their place in the problem on both an individual and a national basis.

5.4 Describe a set of workable tactical solutions that could be implemented individually by FI's to decrease the risk of insider threats.

5.5 Provide a set of strategic direction solutions that could be used by individual FI's and translated into industry-wide policies, standards, processes, and solutions.

5.6 Investigate technologies such as behavioral modeling and social network analysis, as well as advanced information sharing methodologies.

5.7 Investigate application of wireless sensor networks to monitoring and surveillance, e.g. of critical financial and banking center operations. Wireless sensors can control doors, tag computers, operate cameras and other monitoring device to provide security information remotely.

Challenge Project 6
Financial Information Tracing and Policy Enforcement

The Situation

Currently, the Financial Services Industry is dependent upon communications networks and computers that are vulnerable to both outsider hacking and insider attacks aimed at stealing sensitive data to be used for criminal gains, e.g. account takeover, identity theft and other fraudulent acts. Regulatory directives at every level of government and across jurisdictions call for management of sensitive information with respect to appropriate use. Even if the Financial Services were to build a secure infrastructure to protect our financial transactions as addressed in Challenge Project 1, we are still vulnerable to having sensitive information stolen by outside criminals and malicious nation-states who attack less secure systems outside the financial services industries' secure transaction infrastructure with whom we share portions of this information, e.g. merchants and third party vendors.

Impact and timing

The result of these trends, if not checked, would be for customers to lose confidence in the banking system, which has become increasingly dependent on these computer networks and systems. If this situation is not addressed within the next 2-5 years the banking and financial services industry will face critical brand erosion and significant loss of customers, as well as losses realized by their customers. Increasing incidents of privacy breaches will lead to loss of consumer confidence in Financial Services.

The Challenge

6 Define the architecture of a Financial Information System that provides a comprehensive privacy and security model. Such a system should:

6.1 Provide Strong access, authentication and entitlement controls.

6.2 Track information across its entire life cycle, including:

- 6.2.1 Track and provide auditable records of who accessed what information.
- 6.2.2 Track and provide auditable records how the information was used and what actions were taken.

Challenge Project 6
Financial Information Tracing and Policy Enforcement

6.2.3 Track and provide auditable records indicating whether the information or a derivative of this information was shared, with whom it was shared, when and where.

6.2.4 Track and provide auditable records of what subsequent actions were taken and by whom.

6.3 Provide the ability to set and enforce unified policies to prohibit, constrain, or alert attempts at using or sharing information in ways that violate policies.

6.4 Scale to economically support hundreds of billions of records.

6.5 Interoperate with a system that makes information securely accessible across untrustworthy communications networks and computing nodes (see Challenge Project 1).

Challenge Project 7
Testing

The Situation

Much of the software currently used by the Financial Industry has not gone through rigorous software certification and testing. Part of the reason for this is that it is unclear what the benefit would be of this testing. What kinds of tests should be applied? How effective are these tests in catching vulnerabilities? In minimizing the need for patches and patch management? The industry needs a better understanding of the role and the current state of effectiveness of software certification and testing of Financial Services Technology Applications and its underlying infrastructure, i.e. the quantitative impact that a rigorous program of software certification and testing would bring to FI's with respect to the reduction of risk and the avoidance of future costs. Furthermore, this should be related to the types of tests that should be included in a software certification test.

Impact and timing

The cost to the industry of maintaining and upgrading software is growing to the point that it is impeding the Industry from adding badly needed new functionality. Moreover, the inability to keep up with the growing vulnerabilities of our applications software and to keep up with patching these vulnerabilities is leading to an increase in the likelihood of catastrophic failure (for example, a service disruption or highly publicized and damaging loss due to fraud and error).

The Challenge

7 Provide software certification and testing standards that are relevant to the Financial Industry. The results of this research should:

7.1 Evaluate the effectiveness of software certification and testing programs (e.g., common criteria).

7.2 Explore better ways to design and test software during its development to minimize errors and reduce software vulnerabilities.

7.3 Explore ways to design software that can discover vulnerabilities automatically and self-heal, much as the human immune system does today.

Challenge Project 7
Testing

7.4 Work with the Information Technology Industry to apply concepts from the Trusted Computing Initiative to build and protect a core "Trusted Financial Service Processing Layer" upon which our applications can safely be built, and upon which the Financial Industry can fall back on to provide a continuous level of financial service at some minimum essential level in the face of massive failure, attack, or successful fraud.

7.5 Develop better metrics that can help us better understand the effectiveness of our software certification programs.

Challenge Project 8
Standards for measuring ROI of CIP and Security Technology

The Situation

One of the key issues in the adoption of improved protective technologies and processes is the ability of the paying organizations to fully understand both the costs and protective benefits provided. Information protection organizations, as part of their regular business, can effectively evaluate for an organization specific cost elements for various protective programs in terms of operating cost, contracting costs, and the cost of purchasing the needed technology. These organizations are less able to develop the total life cycle costs of the protective programs, often underestimate total costs to the Financial Institution for deploying new controls, and generally exhibit poor performance at determining the total costs that must be born by the business lines that are asked to implement, own, and manage these protective programs long-term. Across the entire Financial Services Industry, the information protection and risk management community is generally not well equipped to accurately or completely define, estimate, calculate, measure, or communicate the benefits that result from protective programs. An equivalent of "Generally Accepted Accounting Principles" (GAAP) used in the accounting community would benefit the risk management community.

The Financial Industry needs research on life cycle costs of CIP and Security Technology and the creation of cost-benefit models that can be adopted within institutions and across the industry.

Impact and timing

A clear and accepted methodology to accurately measure both costs and benefits would speed the deployment of improved security technologies within organizations and across the industry. A standard language and financially certifiable methodology to define, estimate, measure, and communicate costs and benefits would assist all institutions. The sooner the industry adopts a standard cost to benefit approach, the more rapidly information protection will integrated into FI priorities.

Challenge Project 8
Standards for measuring ROI of CIP and Security Technology

The Challenge

8 Develop a standardized methodology for calculating ROI for CIP and Security Technology that is relevant to the Financial Industry. Such a methodology should:

8.1 Develop cost-benefit models describing the costs and benefits of improved CIP and security technology. The output of this research should result in agreement from participating Institutions and the Industry at large for adoption of these models and approaches. This model should include data that are appropriate to estimate the total life cycle cost when implementing individual information protection programs, and form a repository for case studies that may be accessed and used by other institutions.

8.2 Develop common mathematics and rules for estimating program deployment costs that allow Institutions to "plug-in" their specific costs, and that are open to varied implementation approaches.

8.3 Quantify the costs/benefits for information protection as mandated by the Sarbanes-Oxley Act and Gramm-Leach-Bliley Act, and link overall approach to provide reporting to need GLBA, SOX and other regulatory or legal requirements.

8.4 Establish commonly acceptable cost to benefit estimation, measurement, and communication processes and methods for the Financial Industry.

Role of the Banking and Finance Test Bed

Currently, the banking and financial industry relies on individual firms' research and vendor-driven test facilities to provide the information required to make IT business decisions. This testing method has several drawbacks:

- Duplication of resources by individual firms in the Financial Industry.

- Incomplete or context-insensitive data.

- Test beds are vendor- and evaluation-driven, leaving few resources for research devoted to the needs of the industry.

A Banking and Finance Test Bed could overcome these shortcomings. Pooled resources would minimize duplication of effort and expense, and provide an economically efficient forum for participants to gain independent data on existing IT products. The test bed could also be used by researchers who want to evaluate the applicability of their approach within the financial services arena, or to compare multiple approaches to allow the industry to standardize on the best solution using criteria developed by the participants themselves. Research facilities should plan to provide for data collection and consolidation, provide analytic tools and modeling capability to support the analysis of collected data, provide for the development and coordination of hypotheses and for the testing of various hypotheses with Industry participation, and for the presentation and review of project progress and results with sponsors, participants, various communities of interest, and with the Industry.

The Banking and Finance Test Bed could be used in multiples ways to meet the challenges identified in this paper. Some examples include:

- Testing the interoperability and compliance of SFTP- and RFTS-compliant hardware and software.

- Center of expertise in data scrubbing, allowing live transactions captured from the production data stream of Financial Institutions to be cleansed of any private or sensitive information and incorporated into standard data sets.

Role of the Banking and Finance Test Bed

- Testing and certification of COTS components compliance with security practices and standards as may be selected by the Committee.

- Testing the interoperability and compliance of "identity layer"-compliant hardware and software.

- Maintain standard library of fictional identities used as test cases to drive interoperability testing.

- Center of expertise in developing best practices and achieving consensus support.

Financial Services Sector Coordinating Council

www.fsscc.org